

REMARKS

Claims 1-6 are pending. Claims 1, 3, 4, 5 and 6 are rejected under 35 U.S.C. §102(e). Claim 2 is rejected under 35 U.S.C. §103(a). Applicants respectfully traverse these rejections for at least the reasons stated below and respectfully request the Examiner to reconsider and withdraw these rejections.

I. REJECTIONS UNDER 35 U.S.C. §102(e):

The Examiner has rejected claims 1, 3, 4, 5 and 6 under 35 U.S.C. §102(e) as being anticipated by Gales (U.S. Patent Application Publication No. 2003/0084323) (hereinafter "Gales"). Applicants respectfully traverse these rejections for at least the reasons stated below and respectfully request the Examiner to reconsider and withdraw these rejections.

For a claim to be anticipated under 35 U.S.C. §102, each and every claim limitation must be found within the cited prior art reference and arranged as required by the claim. M.P.E.P. §2131.

Applicants respectfully assert that Gales does not disclose "determining a present count of occurrences of an event for a present monitoring period" as recited in claim 1 and similarly in claim 5. The Examiner cites paragraph [0021], lines 1-5 of Gales as disclosing the above-cited claim limitation. Office Action (10/26/2007), page 2. Applicants respectfully traverse.

Gales instead discloses that in operation, the monitor application 40 monitors network traffic and/or usage associated with the nodes 12 and/or server 18 for a predetermined time period. [0021]. Gales further discloses that the monitor application 40 stores the network usage and/or traffic information in the network activity log 52. [0021].

Hence, Gales discloses a monitor application which monitors network traffic and/or usage associated with the nodes and/or the server for a predetermined time period. Gales further discloses that the monitored network usage and/or traffic information is stored in a network activity log.

There is no language in the cited passage that discloses determining a present count of occurrences of an event. Instead, Gales discloses that monitor application 40 monitors and stores network usage and/or traffic information. The Examiner has not pointed to any language in the cited passage that discloses that monitor application 40 counts occurrences of an event for a present monitoring period. Thus, Gales does not disclose all of the limitations of claims 1 and 5, and thus Gales does not anticipate claims 1 and 5. M.P.E.P. §2131.

Applicants further assert that Gales does not disclose "comparing the present count with numbers of occurrences of the event in a plurality of earlier monitoring periods" as recited in claim 1 and similarly in claim 5. The Examiner cites paragraph [0022], lines 1-6 and 11-17; and paragraph [0023], lines 2-5 of Gales as disclosing the above-cited claim limitation. Office Action (10/26/2007), page 2. Applicants respectfully traverse.

Gales instead discloses that after monitoring the network traffic and usage patterns for the predetermined time period, the profile application 42 retrieves the network activity log 52 information and automatically generates an activity profile for the monitored nodes 12 and/or server 18 and stores the profile in the database 50 as the activity profile data 54. [0022]. Gales additionally discloses that the activity profile data 54 may be updated on a substantially continuous or ongoing basis or may be updated in accordance with predefined time periods. [0022]. Further, Gales discloses that for example, the activity profile data 54 may be updated on a daily, weekly, monthly or other predefined time period schedule. [0022]. Furthermore, Gales discloses that the activity profile data 54 may be updated by examining the network activity during a variety of different time periods. [0022]. Additionally, Gales discloses that after generation of the activity profiles for the nodes 12 and/or server 18, future network activity and usage is compared to the activity profile to determine whether particular network activities may be suspicious or potentially harmful activities. [0023].

Hence, Gales discloses that the profile application retrieves the activity log information and generates an activity profile for the monitored nodes and/or the

server. Gales further discloses that the data in the activity profile may be updated on an ongoing basis or in accordance with predefined time periods. Further, Gales discloses that future network activity and usage is compared to the activity profile to determine whether particular network activities may be suspicious or potentially harmful activities.

There is no language in the cited passages that discloses comparing the present count with numbers of occurrences of the event. Instead, Gales discloses comparing the activity profile, which includes network usage and/or traffic information, to the future network activity and usage. There is no comparison being made between a present count with the number of occurrences of the event. Neither is there any language in the cited passages that discloses comparing the present count with numbers of occurrences of the event in a plurality of earlier monitoring periods. Thus, Gales does not disclose all of the limitations of claims 1 and 5, and thus Gales does not anticipate claims 1 and 5. M.P.E.P. §2131.

Applicants further assert that Gales does not disclose "invoking a first action if the present count exceeds a predetermined proportion of the numbers of occurrences of the event in the plurality of earlier monitoring periods" as recited in claim 1 and similarly in claim 5. The Examiner cites paragraph [0023], lines 9-13 and elements 214, 216 in Figure 3 of Gales as disclosing the above-cited claim limitation. Office Action (10/26/2007), page 3. Applicants respectfully traverse.

Gales instead discloses that if the network activity exceeds the activity profile, the recognition engine 44 automatically initiates security or other investigative measures to determine whether the particular network activity may be an unauthorized intrusion or other unauthorized network usage. [0023].

Hence, Gales discloses that if the network activity exceeds the activity profile, then a recognition engine initiates security or other investigative measures.

There is no language in the cited passages that discloses invoking a first action if the present count exceeds a predetermined proportion of the numbers of occurrences of the event. Neither is there any language in the cited passages that discloses invoking a first action if the present count exceeds a predetermined

proportion of the numbers of occurrences of the event in the plurality of earlier monitoring periods. Applicants respectfully request the Examiner to particularly point out in Gales where Gales allegedly discloses the present count, the predetermined proportion of the number of occurrences of the event and the plurality of earlier monitoring periods pursuant to 37 C.F.R. §1.104(c)(2). Thus, Gales does not disclose all of the limitations of claims 1 and 5, and thus Gales does not anticipate claims 1 and 5. M.P.E.P. §2131.

Applicants further assert that Gales does not disclose "an event counter for determining a present count of occurrences of an event for a present monitoring period" as recited in claim 6. The Examiner cites paragraph [0021], lines 1-5 of Gales as disclosing the above-cited claim limitation. Office Action (10/26/2007), page 4. Applicants respectfully traverse.

As stated above, Gales instead discloses a monitor application 40 which monitors network traffic and/or usage associated with nodes 12 and/or server 18 for a predetermined time period. Gales further discloses that the monitored network usage and/or traffic information is stored in a network activity log.

There is no language in the cited passage that discloses an event counter. Neither is there any language in the cited passage that discloses an event counter for determining a present count of occurrences of an event for a present monitoring period. Thus, Gales does not disclose all of the limitations of claim 6, and thus Gales does not anticipate claim 6. M.P.E.P. §2131.

Applicants further assert that Gales does not disclose "a history table for storing numbers of occurrences of the event in earlier monitoring periods" as recited in claim 6. The Examiner cites paragraph [0016], lines 1-4 of Gales as disclosing the above-cited claim limitation. Office Action (10/26/2007), page 4. Applicants respectfully traverse.

Gales instead discloses that the system 30 illustrated in Figure 2 also includes a database 50. [0016]. Gales further discloses that in the illustrated embodiment, the database 50 includes a network activity log 52, activity profile data 54, and a network event log 56. [0016].

The Examiner must provide a basis in fact and/or technical reasoning to support the assertion that either network activity log 52, activity profile data 54, or network event log 56 of Gales discloses a history table for storing numbers of occurrences of the event in earlier monitoring periods. *Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). That is, the Examiner must provide extrinsic evidence that must make clear that either network activity log 52, activity profile data 54, or network event log 56 of Gales discloses a history table for storing numbers of occurrences of the event in earlier monitoring periods, and that it would be so recognized by persons of ordinary skill. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). Since the Examiner has not provided any such objective evidence, the Examiner has not presented a *prima facie* case of anticipation for rejecting claim 6. M.P.E.P. §2112.

Applicants further assert that Gales does not disclose "logic for comparing the present count with numbers of occurrences of the event in a plurality of earlier monitoring periods selected from the history table, invoking a first action if the present count exceeds a predetermined proportion of the numbers of occurrences of the event in the plurality of earlier monitoring periods, and invoking a second action if the present count does not exceed the predetermined proportion of the numbers of occurrences of the event in the plurality of earlier monitoring periods" as recited in claim 6. The Examiner cites paragraph [0014], lines 16-21 and paragraph [0016], lines 1-6 of Gales as disclosing the above-cited claim limitations. Office Action (10/26/2007), page 5. Applicants respectfully traverse.

Gales instead disclose that after the activity profiles have been generated, the recognition engine 44 compares future network events for a particular node 12 to the activity profile corresponding to the node 12. [0014]. Gales further discloses that if the particular network event exceeds the activity profile for the node 12, the network event may be blocked, recorded, allowed, or otherwise processed. [0014]. Additionally, Gales discloses that the database 50 includes a network activity log 52, activity profile data 54, and a network event log 56. [0016].

Hence, Gales discloses comparing future network events for a particular node to the activity profile corresponding to the node. Gales further discloses that if the particular network event exceeds the activity profile for the node, then the network event may be blocked, recorded, allowed, or otherwise processed.

There is no language in the cited passages that discloses logic for comparing the present count with numbers of occurrences of the event. Instead, Gales discloses comparing future network events with an activity profile. Neither is there any language in the cited passages that discloses logic for comparing the present count with numbers of occurrences of the event in a plurality of earlier monitoring periods selected from the history table. Neither is there any language in the cited passages that discloses invoking a first action if the present count exceeds a predetermined proportion of the numbers of occurrences of the event in the plurality of earlier monitoring periods. Instead, Gales discloses that a network event may be blocked, recorded, allowed, or otherwise processed if the particular network event exceeds the activity profile. Neither is there any language in the cited passage that discloses invoking a second action if the present count does not exceed the predetermined proportion of the numbers of occurrences of the event in the plurality of earlier monitoring periods. Thus, Gales does not disclose all of the limitations of claim 6, and thus Gales does not anticipate claim 6. M.P.E.P. §2131.

Claims 3-4 each recite combinations of features of independent claim 1, and hence claims 3-4 are not anticipated by Gales for at least the above-stated reasons that claim 1 is not anticipated by Gales.

Claims 3-4 recite additional features, which, in combination with the features of the claim upon which they depend, are not anticipated by Gales.

For example, Gales does not disclose "wherein the second action includes logging the present count without taking further corrective action" as recited in claim 3. The Examiner cites paragraph [0014], lines 11-15 and paragraph [0016], lines 1-6 of Gales as disclosing the above-cited claim limitation. Office Action (10/26/2007), page 3. Applicants respectfully traverse.

Gales instead discloses that the monitor application 40 monitors network usage associated with each of the nodes 12. [0014]. Gales further discloses that using the established network usage patterns, the profile application 42 generates a network activity profile corresponding to each of the nodes 12. [0014]. Additionally, Gales discloses that the system 30 illustrated in Figure 2 also includes a database 50. [0016]. Gales further discloses that in the illustrated embodiment, the database 50 includes a network activity log 52, activity profile data 54, and a network event log 56. [0016].

Hence, Gales discloses a monitoring application monitoring network usage associated with each of the nodes. Gales further discloses that the profile application generates a network activity profile corresponding to each of the nodes using the established network usage patterns.

There is no language in the cited passages that discloses a second action that includes logging the present count without taking further corrective action. Thus, Gales does not disclose all of the limitations of claim 3, and thus Gales does not anticipate claim 3. M.P.E.P. §2131.

Applicants further assert that Gales does not disclose "wherein the plurality of earlier monitoring periods all begin at the same times on consecutive days previous to the present monitoring period" as recited in claim 4. The Examiner cites paragraph [0022], lines 11-15 of Gales as disclosing the above-cited claim limitation. Office Action (10/26/2007), page 3. Applicants respectfully traverse.

As stated above, Gales instead discloses that the activity profile data 54 may be updated on a substantially continuous or ongoing basis or may be updated in accordance with predefined time periods. [0022]. Further, Gales discloses that the activity profile data 54 may be updated on a daily, weekly, monthly or other predefined time period schedule. [0022]. Furthermore, Gales discloses that the activity profile data 54 may be updated by examining the network activity during a variety of different time periods. [0022].

Hence, Gales discloses that the activity profile data may be updated on a daily, weekly, monthly or other predefined time period schedule.

There is no language in the cited passage that discloses that the plurality of earlier monitoring periods all begin at the same times. Neither is there any language in the cited passage that discloses that the plurality of earlier monitoring periods all begin at the same times on consecutive days previous to the present monitoring period. Thus, Gales does not disclose all of the limitations of claim 4, and thus Gales does not anticipate claim 4. M.P.E.P. §2131.

As a result of the foregoing, Applicants respectfully assert that not each and every claim limitation was found within Gales, and thus claims 1 and 3-6 are not anticipated by Gales. M.P.E.P. §2131.

II. REJECTIONS UNDER 35 U.S.C. §103(a):

The Examiner has rejected claim 2 under 35 U.S.C. §103(a) as being unpatentable over Gales in view of Porras et al. (U.S. Patent Application Publication No. 2004/0010718) (hereinafter "Porras"). Applicants respectfully traverse these rejections for at least the reasons stated below and respectfully request the Examiner to reconsider and withdraw these rejections.

A. Gales and Porras, taken singly or in combination, do not teach at least the following claim limitations.

Applicants respectfully assert that Gales and Porras, taken singly or in combination, do not teach "wherein the predetermined proportion is a majority" as recited in claim 2. The Examiner cites paragraph [0035], lines 1-3 and paragraph [0040] of Porras teaching the above-cited claim limitation. Office Action (10/26/2007), page 6. Applicants respectfully traverse.

Porras instead teaches that the profile engine 22 can use a wide range of multivariate statistical measures to profile network activity indicated by an event stream. [0035]. Porras further teaches that the profile is subdivided into short-term and long-term profiles. [0040]. Furthermore, Porras teaches that the short-term profile accumulates values between updates, and exponentially ages (e.g., weighs data based on how long ago the data was collected) values for comparison to the long-term profile. [0040]. In addition, Porras teaches that as a consequence of the aging mechanism, the short-term profile characterizes recent activity, where "recent" is

determined by a dynamically configurable aging parameters. [0040]. Furthermore, Porras teaches that the long-term profile is itself slowly aged to adapt to changes in subject activity. [0040]. Further, Porras teaches that anomaly scoring compares related attributes in the short-term profile against the long-term profile. [0040].

Hence, Porras teaches an engine that can use a wide range of multivariate statistical measures to profile network activity indicated by an event stream. Porras additionally teaches subdividing a profile into short-term and long-term profiles, where short-term profiles characterize recent activity and long-term profiles characterize older activity. Porras further teaches that the attributes of the short-term profile is compared against the attributes of the long-term profile.

There is no language in the cited passages that teaches that the predetermined proportion of the number of occurrences of the event in the plurality of earlier monitoring periods is a majority. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 2, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

- B. Examiner's reasoning for modifying Gales with Porras to include the missing claim limitation of claim 2 is insufficient to establish a *prima facie* case of obviousness.

Most if not all inventions arise from a combination of old elements. *See In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Obviousness is determined from the vantage point of a hypothetical person having ordinary skill in the art to which the patent pertains. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Therefore, an Examiner may often find every element of a claimed invention in the prior art. *Id.* However, identification in the prior art of each individual part claimed is insufficient to defeat patentability of the whole claimed invention. *See Id.* In order to establish a *prima facie* case of obviousness, the Examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998). The Examiner must provide articulated reasoning with some

rational underpinning to support the legal conclusion of obviousness. *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (cited approvingly in *KSR International Co. v. Teleflex Inc.*, 82 U.S.P.Q.2d 1385, 1396 (U.S. 2007)).

As understood by Applicants, the Examiner admits that Gales does not teach "wherein the predetermined proportion is a majority" as recited in claim 2. Office Action (10/26/2007), page 5. The Examiner asserts that Porras teaches the above-cited claim limitation. *Id.* at pages 5-6. The Examiner's reasoning for modifying Gales with Porras to include the above-cited claim limitation is "in order to filter events to obtain the invention specified in claim 2." *Id.* at page 6. The Examiner's reasoning is insufficient to establish a *prima facie* case of obviousness in rejecting claim 2.

The Examiner appears to cite to paragraphs [0005-0006] of Porras as support for the Examiner's reasoning for modifying Gales with Porras to include the above-cited missing claim limitation of claim 2. Office Action (10/26/2007), page 6. Porras teaches that computer networks offer users ease and efficiency in exchanging information. [0005]. Porras further teaches that unfortunately, the very interoperability and sophisticated integration of technology that makes networks such valuable assets also make them vulnerable to attack. [0006]. Hence, Porras teaches that computer networks offer users ease and efficiency in exchanging information as well as the fact that networks are vulnerable to attack. There is no language in Porras (and in particular paragraphs [0005-0006]) that makes any suggestion to have a predetermined proportion of the number of occurrences of the event in the plurality of earlier monitoring periods be a majority (missing claim limitation) in order to filter events (Examiner's reasoning). The Examiner has to provide some rational connection between the cited passage that is the source of the Examiner's reasoning and the above-cited missing claim limitation. The Examiner's source of reasoning (paragraphs [0005-0006] of Porras) focuses on background information about networks and does not provide reasons as to why one skilled in the art would modify Gales to include the above-cited missing claim limitation of claim 2. Accordingly, the Examiner has not presented a *prima facie* case of obviousness for rejecting claim

2. *KSR International Co. v. Teleflex Inc.*, 82 U.S.P.Q.2d 1385, 1396 (U.S. 2007); *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998).

III. CONCLUSION:

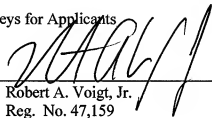
As a result of the foregoing, it is asserted by Applicants that claims 1-6 in the Application are in condition for allowance, and Applicants respectfully request an allowance of such claims. Applicants respectfully request that the Examiner call Applicants' attorney at the below listed number if the Examiner believes that such a discussion would be helpful in resolving any remaining issues.

Respectfully submitted,

WINSTEAD P.C.

Attorneys for Applicants

By: _____


Robert A. Voigt, Jr.
Reg. No. 47,159

P.O. Box 50784
Dallas, TX 75201
(512) 370-2832

Austin_1 519271v.1